

EVALUATING PRIME POWER GAUSS AND JACOBI SUMS

MISTY LONG, VINCENT PIGNO, AND CHRISTOPHER PINNER

ABSTRACT. We show that for any mod p^m characters, χ_1, \dots, χ_k , the Jacobi sum,

$$\sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=B}}^{p^m} \chi_1(x_1) \cdots \chi_k(x_k),$$

has a simple evaluation when m is sufficiently large (for $m \geq 2$ if $p \nmid B$). As part of the proof we give a simple evaluation of the mod p^m Gauss sums when $m \geq 2$.

1. INTRODUCTION

For multiplicative characters χ_1 and χ_2 mod q one defines the classical Jacobi sum by

$$(1) \quad J(\chi_1, \chi_2, q) := \sum_{x=1}^q \chi_1(x) \chi_2(1-x).$$

More generally for k characters χ_1, \dots, χ_k mod q one can define

$$(2) \quad J(\chi_1, \dots, \chi_k, q) = \sum_{x_1=1}^q \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=1}}^q \chi_1(x_1) \cdots \chi_k(x_k).$$

If the χ_i are mod rs characters with $(r, s) = 1$ then, writing $\chi_i = \chi'_i \chi''_i$ where χ'_i and χ''_i are mod r and mod s characters respectively, it is readily seen (e.g. [12, Lemma 2]) that

$$J(\chi_1, \dots, \chi_k, rs) = J(\chi'_1, \dots, \chi'_k, r) J(\chi''_1, \dots, \chi''_k, s).$$

Hence, one usually only considers the case of prime power moduli $q = p^m$.

Zhang & Yao [11] showed that the sums (1) can in fact be evaluated explicitly when m is even (and χ_1, χ_2 and $\chi_1 \chi_2$ are primitive mod p^m). Working with a slightly more general binomial character sum the authors [9] showed that techniques of Cochrane & Zheng [3] can be used to obtain an evaluation of (1) for any $m > 1$ (p an odd prime). Zhang and Xu [12] considered the general case, (2), obtaining (assuming that $\chi, \chi^{n_1}, \dots, \chi^{n_k}$, and $\chi^{n_1+\cdots+n_k}$ are primitive characters modulo p^m)

$$(3) \quad J(\chi^{n_1}, \dots, \chi^{n_k}, p^m) = p^{\frac{1}{2}(k-1)m} \overline{\chi}(u) \chi(n_1^{n_1} \cdots n_k^{n_k}), \quad u := n_1 + \cdots + n_k,$$

Date: October 24, 2014.

2010 Mathematics Subject Classification. Primary: 11L05; Secondary: 11L03, 11L10.

Key words and phrases. Exponential sums, Gauss sums.

when m is even, and when the m, k, n_1, \dots, n_k are all odd

$$(4) \quad J(\chi^{n_1}, \dots, \chi^{n_k}, p^m) = p^{\frac{1}{2}(k-1)m} \overline{\chi}(u^u) \chi(n_1^{n_1} \dots n_{k-1}^{n_{k-1}}) \begin{cases} \varepsilon_p^{k-1} \left(\frac{un_1 \dots n_k}{p} \right), & \text{if } p \neq 2; \\ \left(\frac{2}{un_1 \dots n_k} \right) & \text{if } p = 2, \end{cases}$$

where $\left(\frac{m}{n} \right)$ is the Jacobi symbol and (defined more generally for later use)

$$(5) \quad \varepsilon_{p^m} := \begin{cases} 1, & \text{if } p^m \equiv 1 \pmod{4}, \\ i, & \text{if } p^m \equiv 3 \pmod{4}. \end{cases}$$

In this paper we give an evaluation for all $m > 1$ (i.e. irrespective of the parity of k and the n_i). In fact we evaluate the slightly more general sum

$$J_B(\chi_1, \dots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\dots+x_k=B}}^{p^m} \chi_1(x_1) \cdots \chi_k(x_k).$$

Of course when $B = p^n B'$, $p \nmid B'$ the simple change of variables $x_i \mapsto B' x_i$ gives

$$J_B(\chi_1, \dots, \chi_k, p^m) = \chi_1 \cdots \chi_k(B') J_{p^n}(\chi_1, \dots, \chi_k, p^m).$$

For example $J_B(\chi_1, \dots, \chi_k, p^m) = \chi_1 \cdots \chi_k(B) J(\chi_1, \dots, \chi_k, p^m)$ when $p \nmid B$. From the change of variables $x_i \mapsto -x_k x_i$, $1 \leq i < k$ one also sees that

$$J_{p^m}(\chi_1, \dots, \chi_k, p^m) = \begin{cases} \phi(p^m) \chi_k(-1) J(\chi_1, \dots, \chi_{k-1}, p^m), & \text{if } \chi_1 \cdots \chi_k = \chi_0, \\ 0, & \text{if } \chi_1 \cdots \chi_k \neq \chi_0, \end{cases}$$

where χ_0 denotes the principal character, so we assume that $B = p^n$ with $n < m$.

Theorem 1.1. *Let p be a prime and $m \geq n+2$. Suppose that χ_1, \dots, χ_k are $k \geq 2$ characters mod p^m with at least one of them primitive.*

If the χ_1, \dots, χ_k are not all primitive mod p^m or $\chi_1 \cdots \chi_k$ is not induced by a primitive mod p^{m-n} character, then $J(\chi_1, \dots, \chi_k, p^m) = 0$.

If the χ_1, \dots, χ_k are primitive mod p^m and $\chi_1 \cdots \chi_k$ is primitive mod p^{m-n} , then

$$(6) \quad J_{p^n}(\chi_1, \dots, \chi_k, p^m) = p^{\frac{1}{2}(m(k-1)+n)} \frac{\chi_1(c_1) \cdots \chi_k(c_k)}{\chi_1 \cdots \chi_k(v)} \delta,$$

where for p odd

$$\delta = \left(\frac{-2r}{p} \right)^{m(k-1)+n} \left(\frac{v}{p} \right)^{m-n} \left(\frac{c_1 \cdots c_k}{p} \right)^m \varepsilon_{p^m}^k \varepsilon_{p^{m-n}}^{-1},$$

and for $p = 2$ and $m - n \geq 5$,

$$(7) \quad \delta = \left(\frac{2}{v} \right)^{m-n} \left(\frac{2}{c_1 \cdots c_k} \right)^m \omega^{(2^n-1)v},$$

with ε_{p^m} as defined in (5), the r and c_i as in (11) and (13) or (14) below, and

$$(8) \quad v := p^{-n}(c_1 + \cdots + c_k), \quad \omega := e^{\pi i/4}.$$

For $m \geq 5$ and $m - n = 2, 3$ or 4 the formula (7) for δ should be multiplied by ω , $\omega^{1+\chi_1 \cdots \chi_k(-1)}$ or $\chi_1 \cdots \chi_k(-1) \omega^{2v}$ respectively.

Of course it is natural to assume that at least one of the χ_1, \dots, χ_k is primitive, otherwise we can reduce the sum to a mod p^{m-1} sum. For $n = 0$ and χ_1, \dots, χ_k and $\chi_1 \cdots \chi_k$ all primitive mod p^m our result simplifies to

$$J(\chi_1, \dots, \chi_k, p^m) = p^{\frac{m(k-1)}{2}} \frac{\chi_1(c_1) \cdots \chi_k(c_k)}{\chi_1 \cdots \chi_k(v)} \delta, \quad v = c_1 + \cdots + c_k,$$

with

$$\delta = \begin{cases} 1, & \text{if } m \text{ is even,} \\ \left(\frac{vc_1 \cdots c_k}{p} \right) \left(\frac{-2rc}{p} \right)^{k-1} \varepsilon_p^{k-1}, & \text{if } m \text{ is odd and } p \neq 2, \\ \left(\frac{2}{vc_1 \cdots c_k} \right), & \text{if } m \geq 5 \text{ is odd and } p = 2. \end{cases}$$

In the remaining $n = 0$ case, $p = 2$, $m = 3$ we have $J(\chi_1, \dots, \chi_k, 2^3) = 2^{\frac{3}{2}(k-1)} (-1)^{\lfloor \frac{k}{2} \rfloor}$ where ℓ denotes the number of characters $1 \leq i \leq k$ with $\chi_i(-1) = -1$.

When the $\chi_i = \chi^{n_i}$ for some primitive mod p^m character χ we can write $c_i = n_i c$ (where c is determined by $\chi(a)$ as in (13) or (14)) and we recover the form (3) and (4) with the addition of a factor $\left(\frac{-2rc}{p} \right)^{k-1}$ for $p \neq 2$, m odd, which of course can be ignored when k is odd as assumed in [12].

For completeness we observe that in the few remaining $m \geq n + 2$ cases (6) becomes

$$J_{p^n}(\chi_1, \dots, \chi_k, p^m) = 2^{\frac{1}{2}(m(k-1)+n)} \begin{cases} -i\omega^{k-\sum_{i=1}^k \chi_i(-1)}, & \text{if } m = 3, n = 1, \\ \omega^{\chi_1 \cdots \chi_k(-1)-1-v} \prod_{i=1}^k \chi_i(-c_i), & \text{if } m = 4, n = 1, \\ i^{1-v} \prod_{i=1}^k \chi_i(c_i), & \text{if } m = 4, n = 2. \end{cases}$$

Our proof of Theorem 1.1 involves expressing the Jacobi sum (2) in terms of classical Gauss sums

$$(9) \quad G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x),$$

where χ is a mod p^m character and $e_y(x) := e^{2\pi i x/y}$. Writing (1) in terms of Gauss sums is well known for the mod p sums and the corresponding result for (2) can be found, along with many other properties of Jacobi sums, in Berndt, R. J. Evans and K. S. Williams [1, Theorem 2.1.3 & Theorem 10.3.1] or Lidl-Niederreiter [5, Theorem 5.21]. There the results are stated for sums over finite fields, \mathbb{F}_{p^m} , so it is not surprising that such expressions exist in the less studied mod p^m case. When χ_1, \dots, χ_k and $\chi_1 \cdots \chi_k$ are primitive, Zhang & Yao [11, Lemma 3] for $k = 2$, and Zhang and Xu [12, Lemma 1] for general k , showed that

$$(10) \quad J(\chi_1, \dots, \chi_k, p^m) = \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^m)}.$$

In Theorem 2.2 we obtain a similar expansion for $J_{p^n}(\chi_1, \dots, \chi_k, p^m)$. As we show in Theorem 2.1 the mod p^m Gauss sums can be evaluated explicitly using the method of Cochrane and Zheng [3] when $m \geq 2$.

For $m = n + 1$ (with at least one χ_i primitive) the Jacobi sum is still zero unless all the χ_i are primitive mod p^m and $\chi_1 \cdots \chi_k$ is a mod p character. Then we can say that $|J_{p^n}(\chi_1, \dots, \chi_k, p^m)| = p^{\frac{1}{2}mk-1}$ if $\chi_1 \cdots \chi_k = \chi_0$ and $p^{\frac{1}{2}(mk-1)}$ otherwise, but an explicit evaluation in the latter case is equivalent to an explicit evaluation of the mod p Gauss sum $G(\chi_1 \cdots \chi_k, p)$ when $m \geq 2$.

2. GAUSS SUMS

In order to use the result from [4] we must first define some terms. For p odd let a be a primitive root mod p^m . We define the integers r , and R_j by

$$(11) \quad a^{\phi(p)} = 1 + rp, \quad a^{\phi(p^j)} = 1 + R_j p^j.$$

Note, $p \nmid r$ and for $j \geq i$,

$$(12) \quad R_j \equiv R_i \pmod{p^i}.$$

For a character $\chi_i \pmod{p^m}$ we define c_i by

$$(13) \quad \chi_i(a) = e_{\phi(p^m)}(c_i),$$

with $1 \leq c_i \leq \phi(p^m)$. Note, $p \nmid c_i$ exactly when χ_i is primitive. For $p = 2$ and $m \geq 3$ we need two generators -1 and $a = 5$ for $\mathbb{Z}_{2^m}^*$ and define R_j , $j \geq 2$, and c_i by

$$(14) \quad a^{2^{j-2}} = 1 + R_j 2^j, \quad \chi_i(a) = e_{2^{m-2}}(c_i),$$

with χ_i primitive exactly when $2 \nmid c_i$. Noting that $R_i^2 \equiv 1 \pmod{8}$, we get

$$(15) \quad R_{i+1} = R_i + 2^{i-1} R_i^2 \equiv R_i + 2^{i-1} \pmod{2^{i+2}}.$$

For $j \geq i + 2$ this gives the relationships,

$$(16) \quad R_j \equiv R_{i+2} \equiv R_{i+1} + 2^i \equiv (R_i + 2^{i-1}) + 2^i \equiv R_i - 2^{i-1} \pmod{2^{i+1}}$$

and

$$(17) \quad R_j \equiv (R_{i-1} + 2^{i-2}) - 2^{i-1} \equiv R_{i-1} - 2^{i-2} \pmod{2^{i+1}}.$$

We shall need an explicit evaluation of the mod p^m , $m \geq 2$, Gauss sums. The form we use comes from applying the technique of Cochrane & Zheng [3] as formulated in [8]. For odd p this is essentially the same as [4, §9] but for $p = 2$ seems new. Variations can be found in Odoni [7] and Mauclaire [6] (see also [1, Chapter 1]).

Theorem 2.1. *Suppose that χ is a mod p^m character with $m \geq 2$. If χ is imprimitive, then $G(\chi, p^m) = 0$. If χ is primitive, then*

$$(18) \quad G(\chi, p^m) = p^{\frac{m}{2}} \chi(-cR_j^{-1}) e_{p^m}(-cR_j^{-1}) \begin{cases} \left(\frac{-2rc}{p}\right)^m \varepsilon_{p^m}, & \text{if } p \neq 2, \\ \left(\frac{2}{c}\right)^m \omega^c, & \text{if } p = 2 \text{ and } m \geq 5, \end{cases}$$

for any $j \geq \lceil \frac{m}{2} \rceil$ when p is odd and any $j \geq \lceil \frac{m}{2} \rceil + 2$ when $p = 2$.

For the remaining cases

$$(19) \quad G(\chi, 2^m) = 2^{\frac{m}{2}} \begin{cases} i, & \text{if } m = 2, \\ \omega^{1-\chi(-1)}, & \text{if } m = 3, \\ \chi(-c)e_{16}(-c), & \text{if } m = 4. \end{cases}$$

Here x^{-1} denotes the inverse of $x \pmod{p^m}$, and r , R_j and c are as in (11) and (13) or (14) and ω as in (8).

Proof. When p is odd [8, Theorem 2.1] gives

$$G(\chi, p^m) = p^{m/2} \chi(\alpha) e_{p^m}(\alpha) \left(\frac{-2rc}{p^m}\right) \varepsilon_{p^m}$$

where α is a solution of

$$(20) \quad c + R_J x \equiv 0 \pmod{p^J}, \quad J := \left\lceil \frac{m}{2} \right\rceil,$$

(and zero if no solution exists). If $p \mid c$ there is no solution and $G(\chi, p^m) = 0$. If $p \nmid c$ by (12) we may take $\alpha = -cR_J^{-1} \equiv -cR_j^{-1} \pmod{p^J}$ for any $j \geq J$. If $p = 2$, $m \geq 6$, and χ is primitive, then [8, Theorem 5.1] gives

$$G(\chi, p^m) = 2^{m/2} \chi(\alpha) e_{2^m}(\alpha) \begin{cases} 1, & \text{if } m \text{ is even,} \\ \left(\frac{1 + (-1)^{\lambda_i R_J c}}{\sqrt{2}} \right), & \text{if } m \text{ is odd,} \end{cases}$$

where α is a solution to

$$(21) \quad c + R_J x \equiv 0 \pmod{2^{\lfloor \frac{m}{2} \rfloor}},$$

and $c + R_J \alpha = 2^{\lfloor \frac{m}{2} \rfloor} \lambda$ (and zero if there is no solution or χ is imprimitive). If $2 \nmid c$ and $j \geq J + 2$ then (using (16) and $R_j \equiv -1 \pmod{4}$) we can take

$$\alpha \equiv -cR_J^{-1} \equiv -c(R_j + 2^{J-1})^{-1} \equiv -c(R_j^{-1} - 2^{J-1}) \pmod{2^{J+1}},$$

and

$$\chi(\alpha) e_{2^m}(\alpha) = \chi(-cR_j^{-1}) e_{2^m}(-cR_j^{-1}) \chi(1 - R_j 2^{J-1}) e_{2^m}(c 2^{J-1}),$$

where, checking the four possible $c \pmod{8}$,

$$\left(\frac{1 + (-1)^{\lambda_i R_J c}}{\sqrt{2}} \right) = \left(\frac{1 - i^c}{\sqrt{2}} \right) = \omega^{-c} \left(\frac{2}{c} \right).$$

Now

$$e_{2^m}(c 2^{J-1}) = e_{2^{m-2}}(c 2^{J-3}) = \chi \left(5^{2^{J-3}} \right) = \chi \left(1 + R_{J-1} 2^{J-1} \right),$$

where, since $R_j \equiv R_{J-1} - 2^{J-2} \pmod{2^{J+1}}$,

$$\begin{aligned} (1 - R_j 2^{J-1}) (1 + R_{J-1} 2^{J-1}) &= 1 + (R_{J-1} - R_j) 2^{J-1} - R_j R_{J-1} 2^{2J-2} \\ &\equiv 1 + 2^{2J-3} + R_{J-1} 2^{2J-2} \equiv 1 + R_{2J-3} 2^{2J-3} \pmod{2^m}. \end{aligned}$$

Hence

$$\chi(1 - R_j 2^{J-1}) e_{2^m}(c 2^{J-1}) = \chi \left(5^{2^{2J-5}} \right) = e_{2^{m-2}}(c 2^{2J-5}) = \begin{cases} \omega^c, & \text{if } m \text{ is even,} \\ \omega^{2c}, & \text{if } m \text{ is odd.} \end{cases}$$

One can check numerically that the formula still holds for the 2^{m-2} primitive mod 2^m characters when $m = 5$. For $m = 2, 3, 4$ one has (19) instead of $2i\omega$, $2^{\frac{3}{2}}\omega^2$, $2^2\chi(c)e_{2^4}(c)\omega^c$ (so our formula (18) requires an extra factor ω^{-1} , $\omega^{-1-\chi(-1)}$ or $\chi(-1)\omega^{-2c}$ respectively).

□

We shall need the counterpart of (10) for the $J_{p^n}(\chi_1, \dots, \chi_k)$. We state a less symmetrical version to allow weaker assumptions on the χ_i :

Theorem 2.2. *Suppose that χ_1, \dots, χ_k are characters mod p^m with $m > n$ and χ_k primitive mod p^m . If $\chi_1 \cdots \chi_k$ is a mod p^{m-n} character, then*

$$(22) \quad J_{p^n}(\chi_1, \dots, \chi_k, p^m) = p^n \frac{\overline{G(\chi_1 \cdots \chi_k, p^{m-n})}}{G(\chi_k, p^m)} \prod_{i=1}^{k-1} G(\chi_i, p^m).$$

If $\chi_1 \cdots \chi_k$ is not a mod p^{m-n} character, then $J_{p^n}(\chi_1, \dots, \chi_k, p^m) = 0$.

From well known properties of Gauss sums (see for example Section 1.6 of [1]),

$$(23) \quad |G(\chi, p^j)| = \begin{cases} p^{j/2}, & \text{if } \chi \text{ is primitive mod } p^j, \\ 1, & \text{if } \chi = \chi_0 \text{ and } j = 1, \\ 0, & \text{otherwise,} \end{cases}$$

when $\chi_1 \cdots \chi_k$ is a primitive mod p^{m-n} character and at least one of the χ_i is a primitive mod p^m character we immediately obtain the symmetric form

$$(24) \quad J_{p^n}(\chi_1, \dots, \chi_k, p^m) = \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^{m-n})}.$$

In particular we recover (10) under the sole assumption that $\chi_1 \cdots \chi_k$ is a primitive mod p^m character.

Proof. We first note that if χ is a primitive character mod p^j , $j \geq 1$, then

$$\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \overline{\chi}(A) G(\chi, p^j).$$

Indeed, for $p \nmid A$ this is plain from $y \mapsto A^{-1}y$. If $p \mid A$ and $j = 1$ the sum equals $\sum_{y=1}^p \chi(y) = 0$. For $j \geq 2$ as χ is primitive there exists a $z \equiv 1 \pmod{p^{j-1}}$ with $\chi(z) \neq 1$, (there must be some $a \equiv b \pmod{p^{j-1}}$ with $\chi(a) \neq \chi(b)$, and we can take $z = ab^{-1}$) so

$$(25) \quad \sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \sum_{y=1}^{p^j} \chi(zy) e_{p^j}(Azy) = \chi(z) \sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay)$$

and $\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = 0$.

Hence if χ_k is a primitive character mod p^m we have

$$\begin{aligned} & \overline{\chi}_k(-1) G(\overline{\chi}_k, p^m) \sum_{x_1=1}^{p^m} \cdots \sum_{x_{k-1}=1}^{p^m} \chi_1(x_1) \cdots \chi_{k-1}(x_{k-1}) \chi_k(p^n - x_1 - \cdots - x_{k-1}) \\ &= \overline{\chi}_k(-1) \sum_{x_1=1}^{p^m} \cdots \sum_{x_{k-1}=1}^{p^m} \chi_1(x_1) \cdots \chi_{k-1}(x_{k-1}) \sum_{y=1}^{p^m} \overline{\chi}_k(y) e_{p^m}((p^n - x_1 - \cdots - x_{k-1})y) \\ &= \sum_{\substack{y=1 \\ p \nmid y}}^{p^m} \overline{\chi}_k(-y) e_{p^m}(p^n y) \left(\sum_{x_1=1}^{p^m} \chi_1(x_1) e_{p^m}(-x_1 y) \cdots \sum_{x_{k-1}=1}^{p^m} \chi_{k-1}(x_{k-1}) e_{p^m}(-x_{k-1} y) \right) \\ &= \sum_{\substack{y=1 \\ p \nmid y}}^{p^m} \overline{\chi_1 \cdots \chi_k}(-y) e_{p^m}(p^n y) \left(\sum_{x_1=1}^{p^m} \chi_1(x_1) e_{p^m}(x_1) \cdots \sum_{x_{k-1}=1}^{p^m} \chi_{k-1}(x_{k-1}) e_{p^m}(x_{k-1}) \right) \\ &= \overline{\chi_1 \cdots \chi_k}(-1) \sum_{\substack{y=1 \\ p \nmid y}}^{p^m} \overline{\chi_1 \cdots \chi_k}(y) e_{p^m}(p^n y) \prod_{i=1}^{k-1} G(\chi_i, p^m). \end{aligned}$$

If $m > n$ and $\overline{\chi_1 \dots \chi_k}$ is a mod p^{m-n} character, then

$$\sum_{\substack{y=1 \\ p \nmid y}}^{p^m} \overline{\chi_1 \dots \chi_k}(y) e_{p^m}(p^n y) = p^n \sum_{\substack{y=1 \\ p \nmid y}}^{p^{m-n}} \overline{\chi_1 \dots \chi_k}(y) e_{p^{m-n}}(y) = p^n G(\overline{\chi_1 \dots \chi_k}, p^{m-n}).$$

If $\overline{\chi_1 \dots \chi_k}$ is a primitive character mod p^j with $m-n < j \leq m$, then by the same reasoning as in (25)

$$\sum_{\substack{y=1 \\ p \nmid y}}^{p^m} \overline{\chi_1 \dots \chi_k}(y) e_{p^m}(p^n y) = p^{m-j} \sum_{y=1}^{p^j} \overline{\chi_1 \dots \chi_k}(y) e_{p^j}(p^{j-(m-n)} y) = 0$$

and the result follows on observing that

$$\overline{G(\chi, p^m)} = \overline{\chi}(-1) G(\overline{\chi}, p^m).$$

□

3. PROOF OF THEOREM 1.1

We assume that χ_1, \dots, χ_k are all primitive mod p^m characters and $\chi_1 \dots \chi_k$ is a primitive mod p^{m-n} character, since otherwise from Theorem 2.2 and (23), $J_{p^n}(\chi_1, \dots, \chi_k, p^m) = 0$. In particular we have (24).

Writing $R = R_{\lceil \frac{m}{2} \rceil + 2}$ then by (24) and the evaluation of Gauss sums in Theorem 2.1 we have

$$\begin{aligned} J_{p^n}(\chi_1, \dots, \chi_k, p^m) &= \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \dots \chi_k, p^{m-n})} \\ &= \frac{\prod_{i=1}^k p^{m/2} \chi_i(-c_i R^{-1}) e_{p^m}(-c_i R^{-1}) \delta_i}{p^{(m-n)/2} \chi_1 \dots \chi_k(-v R^{-1}) e_{p^{m-n}}(-v R^{-1}) \delta_s} \\ (26) \quad &= p^{\frac{1}{2}(m(k-1)+n)} \frac{\prod_{i=1}^k \chi_i(c_i)}{\chi_1 \dots \chi_k(v)} \delta_s^{-1} \prod_{i=1}^k \delta_i, \end{aligned}$$

where

$$\delta_i = \begin{cases} \left(\frac{-2rc_i}{p} \right)^m \varepsilon_{p^m}, & \text{if } p \text{ is odd, } p \neq 2, \\ \left(\frac{2}{c_i} \right)^m \omega^{c_i}, & \text{if } p = 2 \text{ and } m \geq 5, \end{cases}$$

and

$$\delta_s = \begin{cases} \left(\frac{-2rv}{p} \right)^{m-n} \varepsilon_{p^{m-n}}, & \text{if } p \text{ is odd,} \\ \left(\frac{2}{v} \right)^{m-n} \omega^v, & \text{if } p = 2 \text{ and } m-n \geq 5, \end{cases}$$

and the result is plain when p is odd or $p = 2$, $m-n \geq 5$.

The remaining cases $p = 2$, $m \geq 5$ and $m-n = 2, 3, 4$, follows similarly using the adjustment to δ_s observed at the end of the proof of Theorem 2.1 .

4. A MORE DIRECT APPROACH

We should note that the Cochrane & Zheng reduction technique [3] can be applied to directly evaluate the Jacobi sums when p is odd and $m \geq n + 2$ instead of the Gauss sums. For example if $b = p^n b'$ with $p \nmid b'$, then from [9, Theorem 3.1] we have

$$\begin{aligned} J_b(\chi_1, \chi_2, p^m) &= \sum_{x=1}^{p^m} \chi_1(x) \chi_2(b-x) = \sum_{x=1}^{p^m} \overline{\chi_1 \chi_2}(x) \chi_2(bx-1) \\ &= p^{\frac{m+n}{2}} \overline{\chi_1 \chi_2}(x_0) \chi_2(bx_0-1) \left(\frac{-2c_2 r b' x_0}{p} \right)^{m-n} \varepsilon_{p^{m-n}}, \end{aligned}$$

where x_0 is a solution to the characteristic equation

$$(27) \quad c_1 + c_2 - c_1 b x \equiv 0 \pmod{p^{\lfloor \frac{m+n}{2} \rfloor + 1}}, \quad p \nmid x(bx-1).$$

If (27) has no solution mod $p^{\lfloor \frac{m+n}{2} \rfloor}$ then $J_b(\chi_1, \chi_2, p^m) = 0$. In particular we see that:

- i. If $p \nmid c_1$ and $p \mid c_2$, then $J_b(\chi_1, \chi_2, p^m) = 0$.
- ii. If $p \nmid c_1 c_2 (c_1 + c_2)$ then

$$J_b(\chi_1, \chi_2, p^m) = \chi_1 \chi_2(b) \chi_1(c_1) \chi_2(c_2) \overline{\chi_1 \chi_2}(c_1 + c_2) p^{\frac{m}{2}} \delta_2.$$

where

$$\delta_2 = \left(\frac{-2r}{p} \right)^m \left(\frac{c_1 c_2 (c_1 + c_2)}{p} \right)^m \varepsilon_{p^m}.$$

- iii. If $p \nmid c_1$ and $b = p^n b'$, $p \nmid b'$ with $n < m - 1$ then $J_b(\chi_1, \chi_2, p^m) = 0$ unless $p^n \parallel (c_1 + c_2)$ in which case writing $w = (c_1 + c_2)/p^n$,

$$J_b(\chi_1, \chi_2, p^m) = \chi_1 \chi_2(b') \frac{\chi_1(c_1) \chi_2(c_2)}{\chi_1 \chi_2(w)} p^{\frac{m+n}{2}} \left(\frac{-2r}{p} \right)^{m-n} \left(\frac{c_1 c_2 w}{p} \right)^{m-n} \varepsilon_{p^{m-n}}.$$

To see (ii) observe that if $p \mid b$, then $J_b(\chi_1, \chi_2, p^m) = 0$, and if $p \nmid b$, then we can take $x_0 \equiv (c_1 + c_2) c_1^{-1} b^{-1} \pmod{p^m}$ (and hence $b x_0 - 1 = c_2 c_1^{-1}$). Similarly for (iii) if $p^n \parallel (c_1 + c_2)$ we can take $x_0 \equiv p^{-n} (c_1 + c_2) c_1^{-1} (b')^{-1} \pmod{p^m}$.

Of course we can write the generalized sum in the form

$$\begin{aligned} J_{p^n}(\chi_1, \dots, \chi_k) &= \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) \sum_{\substack{x_1=1 \\ b := p^n - x_3 - \cdots - x_k}}^{p^m} \chi_1(x_1) \chi_2(b - x_1) \\ &= \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) J_b(\chi_1, \chi_2, p^m), \end{aligned}$$

Hence assuming that at least one of the χ_i is primitive mod p^m (and reordering the characters as necessary) we see from (i) that $J_{p^n}(\chi_1, \dots, \chi_k, p^m) = 0$ unless all the characters are primitive mod p^m . Also when $k = 2$, χ_1, χ_2 primitive, we see from (iii) that $J_{p^n}(\chi_1, \chi_2, p^m) = 0$ unless $\chi_1 \chi_2$ is induced by a primitive mod p^{m-n} character, in which case we recover the formula in Theorem 1.1 on observing that $\left(\frac{c_1 c_2}{p} \right)^n \varepsilon_{p^{m-n}}^2 = \varepsilon_{p^m}^2$; this is plain when n is even, for n odd observe that $\left(\frac{c_1 c_2}{p} \right) = \left(\frac{(c_1 + c_2)^2 - (c_1 - c_2)^2}{p} \right) = \left(\frac{-1}{p} \right)$. We show that a simple induction recovers the formula for all $k \geq 3$. We assume that all the χ_i are primitive mod p^m and

observe that when $k \geq 3$ we can further assume (reordering as necessary) that $\chi_1\chi_2$ is also primitive mod p^m , since if $\chi_1\chi_3, \chi_2\chi_3$ are not primitive then $p \mid (c_1 + c_3)$ and $p \mid (c_2 + c_3)$ and $(c_1 + c_2) \equiv -2c_3 \not\equiv 0 \pmod{p}$ and $\chi_1\chi_2$ is primitive. Hence from (ii) we can write

$$\begin{aligned} J_{p^m}(\chi_1, \dots, \chi_k, p^m) &= \frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(c_1 + c_2)} p^{\frac{m}{2}} \delta_2 \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) \chi_1\chi_2(b) \\ &= \chi_1(c_1)\chi_2(c_2) \overline{\chi_1\chi_2}(c_1 + c_2) p^{\frac{m}{2}} \delta_2 J_{p^n}(\chi_1\chi_2, \chi_3, \dots, \chi_k, p^m). \end{aligned}$$

Assuming the result for $k-1$ characters we have $J_{p^n}(\chi_1\chi_2, \chi_3, \dots, \chi_k, p^m) = 0$ unless $\chi_1 \cdots \chi_k$ is induced by a primitive mod p^{m-n} character in which case

$$J_{p^n}(\chi_1\chi_2, \chi_3, \dots, \chi_k, p^m) = \chi_1\chi_2(c_1 + c_2) \prod_{i=3}^k \chi_i(c_i) \overline{\chi_1 \cdots \chi_k}(v) \delta_3 p^{\frac{m(k-2)+n}{2}}$$

with

$$\delta_3 = \left(\frac{-2r}{p} \right)^{m(k-2)+n} \left(\frac{v}{p} \right)^{m-n} \left(\frac{(c_1 + c_2)c_3 \cdots c_k}{p} \right)^m \varepsilon_p^{k-1} \varepsilon_p^{-1}.$$

Our formula for k characters then follows on observing that $\delta_2\delta_3 = \delta$.

REFERENCES

- [1] B.C. Berndt, R.J. Evans & K.S. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. series of monographs and advanced texts, vol. 21, Wiley, New York 1998.
- [2] T. Cochrane, *Exponential sums with rational function entries*, Acta Arith. 95 (2000), no. 1, 67-95.
- [3] T. Cochrane, Zhiyong Zheng, *Pure and mixed exponential sums*, Acta Arith. 91 (1999), no. 3, 249-278.
- [4] T. Cochrane, Zhiyong Zheng, *A survey on pure and mixed exponential sums modulo prime powers*, Number theory for the millennium, I (Urbana, IL, 2000), 273-300, A K Peters, Natick, MA, 2002.
- [5] R. Lidl & H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its applications 20, 2nd edition, Cambridge University Press, 1997.
- [6] J.-L. Maclaure, *Sommes de Gauss modulo p^α , I & II*, Proc. Japan Acad. Ser. A 59 (1983), 109-112 & 161-163.
- [7] R. Odoni, *On Gauss sums (mod p^n)*, $n \geq 2$, Bull. London Math. Soc. 5 (1973), 325-327.
- [8] V. Pigno & C. Pinner, *Twisted monomial Gauss sums modulo prime powers*, to appear Functiones et Approximatio. (<http://www.math.ksu.edu/~pinner/research.html> preprint 36.)
- [9] V. Pigno & C. Pinner, *Binomial Character Sums Modulo Prime Powers*, submitted to J. Théorie des Nombres de Bordeaux. (<http://www.math.ksu.edu/~pinner/research.html> preprint 38.)
- [10] J. Wang, *On the Jacobi sums mod P^n* , J. Number Theory 39 (1991), 50-64.
- [11] W. Zhang & W. Yao, *A note on the Dirichlet characters of polynomials*, Acta Arith. 115 (2004), no. 3, 225-229.
- [12] W. Zhang & Z. Xu, *On the Dirichlet characters of polynomials in several variables*, Acta Arith. 121 (2006), no. 2, 117-124.

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: milong@math.ksu.edu

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: pignov@math.ksu.edu

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: pinner@math.ksu.edu